



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

5 Patent Application

Applicant(s): Bolle et al.  
Docket No.: YOR920000383US2  
Serial No.: 10/623,926  
10 Filing Date: July 21, 2003  
Group: 3621  
Examiner: Jalatee Worjloh

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Signature: Susan Futura Date: December 13, 2005

Title: Business System and Method Using a Distorted Biometrics

15

APPEAL BRIEF

20 Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

25 Sir:

Applicants hereby appeal the final rejection dated July 12, 2005, of claims 1 through 18 of the above-identified patent application.

30 REAL PARTY IN INTEREST

The present application is assigned to International Business Machines Corporation, as evidenced by an assignment recorded on June 16, 2000 in the United States Patent and Trademark Office at Reel 010926, Frame 0168. The real party in interest is Lenovo Group Limited, One Manhattanville Road, Suite PH, Purchase, New York 10577-2100, which is the beneficiary of an obligation of assignment from the assignee of record, International Business Machines Corporation.

35

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

40

STATUS OF CLAIMS

Claims 1 through 18 are pending in the above-identified patent application. Claims 1-11 and 14-18 remain rejected under 35 U.S.C. §103(a) as being unpatentable over Osuga (United States Patent Number 5,644,645) in view of Black  
5 (United States Patent Publication Number 2002/0025062), and claims 12 and 13 remain rejected under 35 U.S.C. §103(a) as being unpatentable over Osuga and Black, and further in view of Ritter (United States Patent Number 6,657,538).

STATUS OF AMENDMENTS

10 There have been no amendments filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is directed to a method of doing business that transforms a biometric used by a user in a transaction. The transformation creates a  
15 distorted biometric. The distorted biometric is used to authenticate the user to another party without requiring the user to provide actual physical or behavioral characteristics about himself to the other party. (Page 10, line 14, to page 24, line 24.) The authenticating party only stores an identifier (ID number) plus the transformed biometric or its representation. Therefore, no other information about the user can be retrieved from  
20 other business or governmental (biometric) businesses. (Page 24, line 25, to page 27, line 26.)

STATEMENT OF GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-11 and 14-18 are rejected under 35 U.S.C. §103(a) as being  
25 unpatentable over Osuga in view of Black, and claims 12 and 13 are rejected under 35 U.S.C. §103(a) as being unpatentable over Osuga and Black, and further in view of Ritter.

ARGUMENT

30 Claims 1-11 and 14-18 are rejected under 35 U.S.C. §103(a) as being unpatentable over Osuga in view of Black, and claims 12 and 13 are rejected under 35

U.S.C. §103(a) as being unpatentable over Osuga and Black, and further in view of Ritter.

Independent Claims 1, 9, 15, 17 and 18

Regarding claims 1, 9, 15, 17, and 18, the Examiner asserts that Osuga  
5 discloses distorting a digital representation of one or more biometrics of a user (i.e.,  
“fingerprint image”) to create a distorted biometric using one or more transformations, at  
least one of the transformations comprising one or more non-invertible functions (see,  
abstract: “a gray image of a fingerprint image sampled by an image scanner portion is  
compressed by a non-reversible (lossy) coding by a non-reversible mechanism”). The  
10 Examiner acknowledges that Osuga does not expressly disclose that the distorted  
biometric represents a user without revealing the digital representation of the one or more  
biometrics, but asserts that Black discloses comparing, in response to a transaction, the  
distorted biometric with one or more stored distorted biometrics, so that the distorted  
biometric represents a user without revealing the digital representation of the one or more  
15 biometrics (paragraph [0064], lines 4-6, “the image compression employ(s) lossy  
algorithms”).

Appellants note that, as the Examiner acknowledges, both Osuga and  
Black disclose coding/compression utilizing lossy algorithms. Osuga, for example,  
teaches that,

20 in the remote computer system, a gray image of a  
fingerprint image sampled by an image scanner portion (10) is compressed  
by a *non-reversible (lossy) coding* by a non-reversible coding mechanism  
(202) and a skeleton pattern generated by a skeleton generating  
mechanism (201) by inputting the gray image, is compressed by a  
25 reversible (lossless) coding by a reversible coding mechanism (203).  
(Abstract; emphasis added.)

In the text cited by the Examiner, Black teaches that,

30 although the image compression *employ lossy algorithms*,  
the algorithms are tuned for fingerprint recognition. Generally, there is  
little or no difference between the original and the decompressed images.  
(Paragraph 0064; emphasis added.)

As Appellants noted in the Amendment and Response to Office Action  
35 dated April 18, 2005, biometric signals are never exactly the same from one presentation

sample to the next and, hence, an “approximate” biometric matcher must be able to handle the small variations, as would be apparent to a person of ordinary skill in the art. Identification and authentication systems typically allow for such “loss” when the biometric information is decompressed and utilized for authenticating or identifying an individual. Thus, while a lossy compression algorithm may not be able to be decompressed to exactly generate the original data, the *biometric information is still revealed in the compressed (distorted) image*, and may be utilized for authentication or identification purposes, as would be apparent to a person of ordinary skill in the art. Thus, *a lossy compression algorithm is invertible in the context of the present invention* and would not allow the present invention to operate properly. Independent claim 1, for example, requires distorting in a processor a digital representation of one or more biometrics of a user to create a distorted biometric using one or more transformations, at least one of the transformations comprising one or more *non-invertible functions*; and comparing, in response to a transaction, the distorted biometric with one or more stored distorted biometrics, *so that the distorted biometric represents a user without revealing the digital representation of the one or more biometrics*.

Thus, Osuga and Black, alone or in combination, do not disclose or suggest distorting in a processor a digital representation of one or more biometrics of a user to create a distorted biometric using one or more transformations, at least one of the transformations comprising one or more non-invertible functions; and comparing, in response to a transaction, the distorted biometric with one or more stored distorted biometrics, so that the distorted biometric represents a user without revealing the digital representation of the one or more biometrics, as required by independent claim 1, do not disclose or suggest wherein said one or more distorted biometrics were created using one or more transformations of a digital representation of one or more biometrics of a user, at least one of the transformations comprising one or more non-invertible functions; and comparing in a processor the one or more requests with one or more of the records, as required by independent claim 9, do not disclose or suggest wherein said distorted biometric was created using one or more transformations of a digital representation of one or more biometrics of a user, at least one of the transformations comprising one or more non-invertible functions, and verifying the identity of the user by comparing in a

processor the received user identifier with a stored user identifier and comparing the received distorted biometric with a stored distorted biometric associated with the stored user identifier, as required by claim 15, do not disclose or suggest sending a user identifier and an associated digital representation of a user biometric to a remote  
5 computer that distorts the digital representation of the user biometric to a distorted biometric using one or more transformations, at least one of the transformations comprising one or more non-invertible functions; and determining in a processor that the user identifier is associated with the distorted biometric and sending an acknowledgment to the financial company, as required by independent claim 17, and do not require  
10 sending a transaction request, a user identifier, and a distorted biometric determined in a processor using one or more transformations that transform a digital representation of one or more biometrics of a user to the distorted biometric, at least one of the transformations comprising at least one non-invertible function; and receiving an authorization for a transaction defined by the transaction request, as required by independent claim 18.

15 Additional Cited References

Ritter was also cited by the Examiner for its disclosure that the distorted biometric is cancelled by allowing a user to replace the distorted biometric with a second distorted biometric. Appellants note that Ritter is directed to a method for authenticating persons, wherein video information of certain body features associated with a user or a  
20 user group is recorded in a point of presence (POP), and such recorded video information is processed to derive biometric keys, which are stored in tables of a biometric server and in a SIM-card of the user. (See, Abstract.) Ritter, however, does not address the issue of distorting biometrics using one or more transformations, at least one of the transformations comprising one or more non-invertible functions.

25 Thus, Ritter does not disclose or suggest distorting in a processor a digital representation of one or more biometrics of a user to create a distorted biometric using one or more transformations, at least one of the transformations comprising one or more *non-invertible functions*; and comparing, in response to a transaction, the distorted biometric with one or more stored distorted biometrics, so that the distorted biometric  
30 represents a user without revealing the digital representation of the one or more biometrics, as required by independent claim 1, does not disclose or suggest wherein said



one or more distorted biometrics were created using one or more transformations of a digital representation of one or more biometrics of a user, at least one of the transformations comprising one or more non-invertible functions; and comparing in a processor the one or more requests with one or more of the records, as required by independent claim 9, does not disclose or suggest wherein said distorted biometric was created using one or more transformations of a digital representation of one or more biometrics of a user, at least one of the transformations comprising one or more non-invertible functions, and verifying the identity of the user by comparing in a processor the received user identifier with a stored user identifier and comparing the received distorted biometric with a stored distorted biometric associated with the stored user identifier, as required by claim 15, does not disclose or suggest sending a user identifier and an associated digital representation of a user biometric to a remote computer that distorts the digital representation of the user biometric to a distorted biometric using one or more transformations, at least one of the transformations comprising one or more non-invertible functions; and determining in a processor that the user identifier is associated with the distorted biometric and sending an acknowledgment to the financial company, as required by independent claim 17, and does not require sending a transaction request, a user identifier, and a distorted biometric determined in a processor using one or more transformations that transform a digital representation of one or more biometrics of a user to the distorted biometric, at least one of the transformations comprising at least one non-invertible function; and receiving an authorization for a transaction defined by the transaction request, as required by independent claim 18.

Consequently, Appellants respectfully submit that independent claims 1, 9, 15, 17, and 18 are patentable over Osuga, Black, and Ritter, alone or in combination.

Claims 12 and 13

Claims 12 and 13 are rejected under 35 U.S.C. §103(a) as being unpatentable over Osuga and Black, and further in view of Ritter. Regarding claims 12 and 13, the Examiner asserts that Ritter discloses that the “biometric is cancelled by allowing a user to replace the distorted biometric with a second distorted biometric (col. 4, lines 9-15).

In the text cited by the Examiner, Ritter teaches that,

5 moreover, it is also possible to offer further services in the POP 9, particularly services for updating biometric keys, for instance because of changes due to aging, or services for completing or adding additional biometric keys or other security information, which further services can be implemented by one skilled in the art according to the above descriptions.  
(Col. 4, lines 9-15.)

10 While Ritter may disclose “updating biometric keys,” Ritter does not disclose or suggest that a *distorted biometric is canceled* by allowing a user to replace the distorted biometric with a second distorted biometric, and does not disclose or suggest where the second distorted biometric is created by a second distortion transform that is  
15 *different than a first distortion transform* used to create the distorted biometric. Claim 12 requires that a distorted biometric is canceled by allowing a user to replace the distorted biometric with a second distorted biometric, and claim 13 requires that a distorted biometric is canceled by allowing a user to replace the distorted biometric with a second distorted biometric, where the second distorted biometric is created by a second distortion transform that is different than a first distortion transform used to create the  
20 distorted biometric.

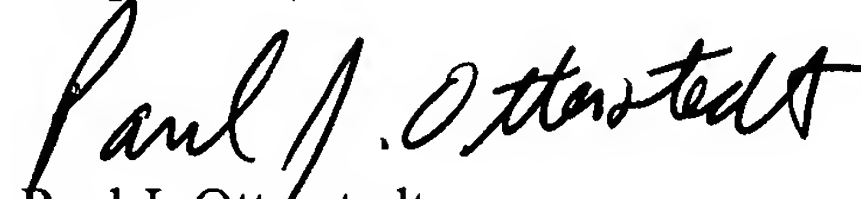
Thus, Osuga, Black, and Ritter, alone or in any combination, do not disclose or suggest that a distorted biometric is canceled by allowing a user to replace the distorted biometric with a second distorted biometric, as required by claim 12, and do not disclose or suggest where the second distorted biometric is created by a second distortion  
25 transform that is different than a first distortion transform used to create the distorted biometric, as required by claim 13.

#### Conclusion

30 The rejections of the cited claims under section 103 in view of Osuga, Black, and Ritter, alone or in any combination, are therefore believed to be improper and should be withdrawn. The remaining rejected dependent claims are believed allowable for at least the reasons identified above with respect to the independent claims.

The attention of the Examiner and the Appeal Board to this matter is appreciated.

Respectfully,



Paul J. Otterstedt  
Attorney for Applicant(s)  
Reg. No. 37,411  
Ryan, Mason & Lewis, LLP  
1300 Post Road, Suite 205  
Fairfield, CT 06824  
(203) 255-6560

Date: December 13, 2005



APPENDIX

1. A method of doing business comprising the steps of:  
distorting in a processor a digital representation of one or more biometrics  
5 of a user to create a distorted biometric using one or more transformations, at least one of  
the transformations comprising one or more non-invertible functions; and  
comparing, in response to a transaction, the distorted biometric with one  
or more stored distorted biometrics, so that the distorted biometric represents a user  
without revealing the digital representation of the one or more biometrics.  
10
2. A method, as in claim 1, where the biometric is a physical characteristic.
3. A method, as in claim 1, where the biometric is a behavioral characteristic.
- 15 4. A method, as in claim 1, where the biometric includes any one or more of  
the following: one or more fingerprints, one or more minutiae, a voice pattern, a facial  
image, an iris, a hand signature, a auditory signature, a gesture, and a gait.
5. A method, as in claim 1, where the transaction is for one or more of the  
20 following: use of a financial instrument, providing a service, executing a contract, a sale,  
a bid, a submitted account number, an authorization, an identification, a reservation  
request, a purchase, a quote, an access to a physical structure, an access to a financial  
account, an authority to manipulate a financial account, an access to a database, an access  
to information, a request for a privilege, a request for a network service, an offer for a  
25 network service, an auction, and an enrollment.
6. A method, as in claim 1, where the distorted biometric is used to  
authenticate the user.
- 30 7. A method, as in claim 1, where the user is any one or more of the  
following: a customer, a customer submitting an order on a network, a client, an  
employee, a user of a service, and a purchaser of a product.

8. A method, as in claim 1, being performed by any one or more of the following: the user, a company, a service company, a company selling products, a bank, a computer, and a credit card company.

5 9. A method of doing business comprising the steps of:  
receiving one or more distorted biometrics associated with a user identifier, wherein said one or more distorted biometrics were created using one or more transformations of a digital representation of one or more biometrics of a user, at least one of the transformations comprising one or more non-invertible functions;  
10 storing a plurality of records in one or more databases, each record having one or more distorted biometrics and a user identifier; and  
receiving one or more requests from a requester, the one or more requests containing one or more target distorted biometrics associated with a target identifier;  
comparing in a processor the one or more requests with one or more of the  
15 records; and  
providing the requester with an indication that the target distorted biometric and the target identifier matched one or more of the respective one or more distorted biometrics and associated user identifiers.

20 10. A method, as in claim 9, further comprising the step of storing a distortion transform used to create the distorted biometric from the digital representation of the one or more biometrics of the user.

11. A method, as in claim 9, where the distorted biometric can not be inverted  
25 to a digital representation of the biometric from which the distorted biometric was created.

12. A method, as in claim 9, where the distorted biometric is canceled by allowing a user to replace the distorted biometric with a second distorted biometric.

30

13. A method, as in claim 12, where the second distorted biometric is created by a second distortion transform that is different than a first distortion transform used to create the distorted biometric.

5 14. A method, as in claim 9, where the requester is any one or more of the following: a financial company, a bank, a brokerage, a credit card company, and a merchant.

15. A method of granting authorization of a transaction, the method  
10 comprising the steps of:

receiving a user identifier, a distorted biometric and a transaction request, wherein said distorted biometric was created using one or more transformations of a digital representation of one or more biometrics of a user, at least one of the transformations comprising one or more non-invertible functions;

15 checking the user identifier with information about one or more accounts of the user;

verifying the identity of the user by comparing in a processor the received user identifier with a stored user identifier and comparing the received distorted biometric with a stored distorted biometric associated with the stored user identifier; and

20 granting authorization for the transaction request if the information about the account is in good standing and the distorted biometric is associated with the user, wherein said distorted biometric was created using the one or more transformations.

16. A method, as in claim 15, where the identity of the user is verified by  
25 receiving an acknowledgment from a remote computer that the user identifier is associated with the digital representation of the distorted biometric.

17. A method of doing business comprising the steps of:  
sending a user identifier and an associated digital representation of a user  
30 biometric to a remote computer that distorts the digital representation of the user biometric to a distorted biometric using one or more transformations, at least one of the

transformations comprising one or more non-invertible functions;

sending the user identifier and a transaction request to a financial company;

determining in a processor that the user identifier is associated with the distorted biometric and sending an acknowledgment to the financial company; and

receiving an authorization for the transaction request from the financial company if the acknowledgment is sent and the user identifier is associated with an account in good standing.

10 18. A method of doing business comprising the steps of:

sending a transaction request, a user identifier, and a distorted biometric determined in a processor using one or more transformations that transform a digital representation of one or more biometrics of a user to the distorted biometric, at least one of the transformations comprising at least one non-invertible function; and

15 receiving an authorization for a transaction defined by the transaction request.

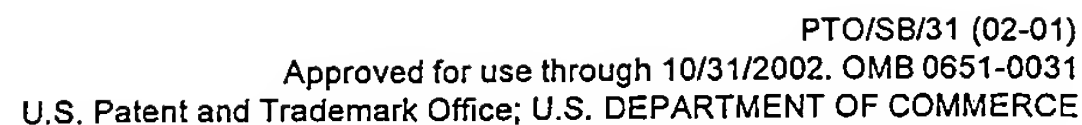
EVIDENCE APPENDIX

There is no evidence submitted pursuant to § 1.130, 1.131, or 1.132 or entered by the Examiner and relied upon by appellant.

RELATED PROCEEDINGS APPENDIX

There are no known decisions rendered by a court or the Board in any proceeding identified pursuant to paragraph (c)(1)(ii) of 37 CFR 41.37.





Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.